LÍNEA DE ACTUACIÓN 3.6: REFUERZO EN CIBERSEGURIDAD

CONTEXTO Y DIAGNÓSTICO

Se entiende por ciberseguridad en el transporte el conjunto de medidas y sistemas enfocados a prevenir las amenazas que llegan al transporte e infraestructuras utilizando como medio de ataque los sistemas de información de los distintos actores que intervienen en el transporte.

Actualmente, por parte del MITMA, se están implantando programas de ciberseguridad en todos los ámbitos del transporte; siendo ésta un **área en constante evolución** y que requiere adaptarse a los cambios tecnológicos en coordinación con otros organismos. Los avances realizados por este Ministerio y sus entidades asociadas han sido numerosos en los últimos años, pero aún es necesario un esfuerzo adicional, dada la rapidez evolutiva del sector.

Por otro lado, hay que señalar que el intercambio de información está cada vez más presente en el funcionamiento de las infraestructuras y en la operativa de transportes, por lo que protegerse frente a posibles amenazas en los sistemas de información es clave desde el punto de vista del mantenimiento de unos niveles óptimos de seguridad y servicio.

Por estas razones, las necesidades en esta materia para el futuro cercano se enmarcan en el refuerzo de la ciberseguridad.

En este sentido las necesidades del sistema de transporte en lo concerniente a ciberseguridad se agrupan en las siguientes líneas principales:

- La creación de un coordinador en políticas de ciberseguridad en un ámbito tan capital como es la seguridad de las infraestructuras críticas.
- La creación y mejora de infraestructuras de ciberseguridad, como son los denominados Centros de Operaciones de Seguridad (o SOC: *Security Operations Centre* por sus siglas en inglés).
- El establecimiento y normalización de operativa mediante planes de ciberseguridad.

Adicionalmente, esta línea de actuación recogerá también las medidas en materia de seguridad vial propuestas en colaboración con la Dirección General de Tráfico.

El objetivo de esta línea de actuación es el refuerzo de las infraestructuras y operativa en un ámbito clave para la seguridad y nivel de servicio de los distintos modos de transporte, como es la Ciberseguridad.

Se pretende llevar a cabo un esfuerzo organizativo y de innovación importante para la puesta en marcha de las medidas incluidas en esta línea de actuación.

MEDIDAS PROPUESTAS

MEDIDA 3.6.1: CREACIÓN DE UN COORDINADOR DE POLÍTICAS DE CIBERSEGURIDAD, RELACIONADAS CON INFRAESTRUCTURAS CRÍTICAS

Se propone la creación de un ente de coordinación de políticas de ciberseguridad, dentro del MITMA, que integre todos los modos de transporte y centre su actividad en la ciberprotección de las infraestructuras definidas en el área estratégica de Transportes del Catálogo Nacional de Infraestructuras Críticas.

Esta figura de coordinación de actuaciones en el ámbito del Ministerio se desarrollará teniendo en cuenta su integración en el esquema definido en el marco del Reglamento de Protección de las Infraestructuras Críticas, y en concreto en sus relaciones con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), así como de la Ley de Seguridad en Redes y Sistemas de Información, adicionalmente con la OCC (Oficina de Coordinación de Ciberseguridad) y con la legislación del Esquema Nacional de Seguridad, con el CCN (Centro Criptológico Nacional dependiente del Centro Nacional de Inteligencia).

MEDIDA 3.6.2: REVISIÓN Y REFUERZO DE LOS MODELOS DE GESTIÓN DE LA CIBERSEGURIDAD EN TODOS LOS MODOS DE TRANSPORTE

Se propone el establecimiento de un Plan de consolidación y/o creación y puesta en marcha de Centros de Operaciones de Seguridad e implantación y/o actualización de planes de ciberseguridad en los sectores ferroviario, marítimo, aéreo y terrestre comercial; de tal forma que se posibilite su integración dentro de los principales organismos encargados de la gestión de la operativa en los diferentes modos (Enaire, Aena, Adif, Puertos del Estado, Renfe, etc.).

Puertos del Estado va a licitar un Centro de Operaciones de Seguridad para dotar a todos los puertos de interés general con un servicio de gestión de incidentes cibernéticos. En algunos de los organismos como Enaire y Renfe (que dispone, desde el año 2014, de un Centro de Operaciones de Seguridad y un Centro de Respuesta ante incidentes de Seguridad), ya se han creado este tipo de centros, por lo que la aplicación de la experiencia adquirida a otros organismos y modos, así como el crecimiento en capacidades y su consolidación será clave. Supondrá un salto cualitativo en la protección frente a amenazas de ciberseguridad, al tener un organismo operativo específico, y planes operativos reglados y actualizados en la materia.

Estos Centros de Operaciones de Seguridad se apoyarán en servicios multi-nube, que permitirán minimizar costes de requisitos comunes de seguridad y dotarán al Grupo MITMA de una plataforma tecnológica de seguridad y que permitirán disponer de un punto central de trazabilidad y autenticación.